



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,373	11/16/2001	Paul England	MS1-954US	5760

22801 7590 06/28/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER

WRIGHT, NORMAN M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 06/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/993,373	Applicant(s) ENGLAND ET AL.	
	Examiner Norman M. Wright	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 April 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3 and 5-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 5-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.


Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

The examiner acknowledges the cancellation of claim 4.

Claim Rejections - 35 USC § 112

The rejection of claim 6 is withdrawn.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-3, 5-15, 17-21, 23-28, 30-32, 34-36, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over England, U.S. Pat. No. 6,757,824, hereinafter '824, and further in view of Chiles, U.S. Pat. No. 6,167,567, hereinafter '567.

As per claims 1-2 '824 teaches a client-side boot domains and boot rules for loading software components into a verified and trusted operating system comprising: receiving a request to upgrade/correct a current trusted core of an operating system (o/s), loading a new o/s, allowing the new core to access application data (figs. 2-5, 7A-7B, summary, col. 2, lines 19 et seq., col. 7, lines 58 et seq., col. 8, lines 1-12 et seq.). Allowing only if it can be verified as the expected trusted core/identify for o/s - boot block and certificates (col. 7, lines 47-55 et seq.). Not explicitly taught is the certification

Art Unit: 2134

authority allowing the action to occur only if the new trusted core has an increasing version number.

Chiles '567, teach allowing an automatic update of software from an certification authority whereby it must have a increasing/updated version number (see abstract, figs. 1-6, summary, and col. 3, lines 63- col. 4, lines 65 et seq., and col. 13, lines 42-45 et seq.). It would have been obvious to one of ordinary skill in the art at the time of the invention to augment the invention of '824 with a version management means as disclosed by '567. One of ordinary skill in the art would have been able to perform this modification by utilizing either firmware, software and/or hardware as taught by '567. One of ordinary skill in the art would have been motivated to perform such a modification because, a person of ordinary skill in the art would have realized that a user seeking to retrieve an update for software for a device or program, may choose the incorrect update or miss intermediate updates, as a result the programs or systems may become corrupt and operate erratically or not at all. Therefore, a person of ordinary skill in the art would have sought to have a means of providing for updates automatically whereby the program and computers systems determine the validity and conditions of the update.

As per claims 3, '824 teach identifying a digest of the new trusted core, having a key, retrieved by new core (figs. 1B and 7B-8B, col. 6, lines 1-19 and 40-65 et seq.).

As per claims 5-8, checking the trusted core, and saving a key if conditions are met (col. 7, lines 47 et seq.). As understood, '824 teach utilizing a generated key (gatekeepers storage key, a hive key and a subset of data for securely storing trusted

applications/ for sealing and unsealing secrets (col. 10, lines 55 et seq. – col. 11, lines 10 et seq.). The generated key/secret/ identity is utilized as part of the encryption to securely store applications for use after upgrading (col. 12, lines 25 et seq.); alternatively, termed a binding key and a key. Allowing only the new core to retrieve new data after the update.

As per claim 9, allowing the new trusted and trusted cores to obtain keys used for securely storing application data (col. 11, lines 1-5 et seq.).

As per claims 31-32, 34-36, and 38, they recite similarly rejected claims features accordingly see above for the specifics of the rejection.

As per claims 10-15, 17-21, 23-24 they distinguish over rejected claims 1-9, by reciting said computer method being contained on a computer readable media having instructions contained therein (see col. 2, lines 57 et seq., col. 5, lines 45 et seq.), and renaming the keys – a key and a binding key respectively, which allows only the new core to retrieve the new data stored after the update.

As per claims 18-21, 23-24, '824 teach the use of random numbers/ nonce as part of the authentication and verification process (col. 7, lines 58 et seq.). He also teaches a method of allowing the key to be calculated by the new trusted core but not vice versa (see cols. 7-8). He teaches sequential identifying new trusted cores for updates (col. 7, lines 57 et seq.).

As per claims 25-28, and 30, they distinguish over previously rejected method of claims 1-21 and 23-24 by reciting a system. '824 teach a system for performing said

Art Unit: 2134

method of claims 1-21 and 23-24, having a processor, a memory, a digest, and keys (see '824 at figs. 1-2).

3. Claims 1-3, 5-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over England, U.S. Pat. No. 6,327,652, hereinafter '652, and further in view of Chiles, U.S. Pat. No. 6,167,567, hereinafter '567.

Alternatively and additionally, '652 teach the limitations found in claims 1-3, and 5-15, 17-21, 23-28, 30-32, 34-36, and 38, he teach a client-side boot domains and boot rules for loading software components into a verified and trusted operating system comprising: receiving a request to upgrade/correct a current trusted core of an operating system (o/s), loading a new o/s, allowing the new core to access application data. Allowing only if it can be verified as the expected trusted core/identify for o/s - boot block and certificates, identifying a digest of the new trusted core, having a key, retrieved by new core, checking the trusted core, and saving a key if conditions are met, utilizing a generated key (gate keepers storage key, hive key, binding key, and a subset of data for securely storing applications/ for sealing and unsealing secrets/applications, where the generated key/secret/ identity is utilized as part of the encryption to securely store applications for use after upgrading, allowing the new trusted and trusted cores to obtain keys used for securely storing application data, said computer method being contained on a computer readable media having instructions contained therein, the use of random numbers/ nonce/seed value/ sentinel, as part of the authentication and verification process, allowing the key to be calculated by the new trusted core but not vice versa, allowing both core access to the data prior to updates and only the new core

Art Unit: 2134

subsequent to updates, sequential identifying new trusted cores for updates, a system for performing said method of claims 1-21 and 23-24, having a processor, a memory, a digest, and keys, see above paragraph 6 for the specifics. Not explicitly taught is the certification authority allowing the action to occur only if the new trusted core has an increasing version number.

Chiles '567, teach allowing an automatic update of software from an certification authority whereby it must have a increasing/updated version number (see abstract, figs. 1-6, summary, and col. 3, lines 63- col. 4, lines 65 et seq., and col. 13, lines 42-45 et seq.). It would have been obvious to one of ordinary skill in the art at the time of the invention to augment the invention of '824 with a version management means as disclosed by '567. One of ordinary skill in the art would have been able to perform this modification by utilizing either firmware, software and/or hardware as taught by '567. One of ordinary skill in the art would have been motivated to perform such a modification because, a person of ordinary skill in the art would have realized that a user seeking to retrieve an update for software for a device or program, may choose the incorrect update or miss intermediate updates, as a result the programs or systems may become corrupt and operate erratically or not at all. Therefore, a person of ordinary skill in the art would have sought to have a means of providing for updates automatically whereby the program and computers systems determine the validity and conditions of the update.

As per claims 16, 22, 29, 33, 35-43, '652 teaches loading and identifying a digital rights management system operating system comprising: a method, system and

computer readable media having an encrypted gatekeeper storage key, a trusted core operating system 'o/s', computing device, store secrets for applications, obtaining the decrypted gatekeeper storage key, allowing both cores access to the data prior to the update but only the new core subsequent to an update, a digest of a new trusted core, generating a new gatekeeper storage key, upgrading applications, identifying a digest, another trusted core, a temporary gatekeeper storage key, a subset of data, a [comparison] of same digest, readable media, a set of keys, a first key, a second key, additional keys, generate temporary/ ephemeral keys, binding key, key, hive key, binding and gatekeeper key, a concatenation operation of a value, key, and trusted core number, and hashing. See (abs., sum. et seq., figs. 1A-8, figs. 10-11, col. 3, lines 65 – col. 4, lines 40 et seq., col. 5, lines 45-56 et seq., col. 7, lines 45 et seq., cols. 8-10, col. 11, lines 30- col. 12, lines 64, cols. 13-14, col. 15, line 29- 66 et seq., col. 16, lines 35- 67, and col. 17, lines 1- col. 18, lines 33 et seq.).

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Norman M. Wright whose telephone number is (571) 272-3844. The examiner can normally be reached on weekdays, from 8AM to 4 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status Information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Norman M. Wright
Primary Examiner
Art Unit 2134